

RECEIVED  
CENTRAL FAX CENTER

AUG 16 2006

## REMARKS

1. Introduction

In the Office Action mailed May 16, 2006, the Examiner rejected claims 1-20 under 35 U.S.C. § 102(b) as being anticipated by Gleichauf et al., U.S. Patent 6,301,668 ("Gleichauf"). Applicants request reconsideration and allowance of the rejected claims for the reasons set forth below.

2. Response to the Claim Rejections

Of the rejected claims, claims 1, 4, 10, 11, 15, 17, and 18 are independent. The Examiner rejected each of these claims and their corresponding dependent claims under 35 U.S.C. § 102(b) as being unpatentable over Gleichauf. In response, Applicants submit that the rejection is improper and should be withdrawn because the Examiner's cited reference does not teach each and every element of the claims, as set forth below.

(a) Claims 1-3

Claim 1 recites "a network reference model for use in configuring security software on a computer network" comprising, *inter alia*, (1) "a database engine providing deduction" and (2) "a security goal database associated with the database engine and describing uses that the hardware and software installed on the network may support." Applicants submit that Gleichauf does not show or suggest the claimed elements for the following reasons.

Gleichauf, col. 5, lines 33-67 does not disclose "a database engine providing deduction." The "database engine providing deduction" in Applicants' claim 1 is part of a "network reference model for use in configuring security software on a computer network." In general, the "database engine providing deduction" is able to use information from other databases (e.g. the claimed

“network information database” and “security goal database”) in conjunction with its deduction capabilities to generate detailed “security goals” that “can then be used by various configuration modules to configure security software packages installed within the network.” (See Applicants’ Specification, paragraph 0007.) In contrast, the Examiner’s cited sections of Gleichauf disclose a “network security system...operable [to] detect attacks upon [an] internal network” by “monitoring traffic on [a] network backbone and performing analysis tasks upon the monitored traffic in the context of network information discovered from [an] internal network.” (See Gleichauf, col. 5, lines 43-48). “[To] detect attacks upon [an] internal network,” Gleichauf further discloses a “scan engine” that “gathers the network information” through various means and a “protocol engine” and a “signature engine” that “perform the analysis tasks upon the monitored traffic.” (See Gleichauf, col. 5, lines 48-51). Gleichauf’s “network security system” that uses a “scan engine,” a “protocol engine,” and a “signature engine” for the purpose of detecting attacks on the network is fundamentally different than Applicants’ “database engine providing deduction” for the purpose of configuring network security software packages.

Gleichauf, col. 7, lines 20-65 does not disclose “a security goal database associated with the database engine” for at least the reason that Gleichauf does not show or suggest a “database engine providing deduction.” Additionally, Gleichauf, col. 7, lines 20-65 describes a “network security system” using a “scan engine” that “sends requests upon [the] network” and “analyzes responses to such requests to discover network information” such as “devices, operating systems, and services on [the] network.” A scan engine that discovers devices, operating systems, and services as they are configured is not the same as “a security goal database that describes uses that the hardware and software on the network may support.”

Therefore, Applicants submit that Gleichauf does not show or suggest all of the elements recited in claim 1. Accordingly, Applicants submit that claim 1 is allowable over Gleichauf for at least the reasons above. Claims 2-3 depend from claim 1. Applicants further submit that claims 2-3 are allowable for at least the reason that they depend from an allowable claim.

**(b) Claims 4-9, and Claim 10**

Claims 4 and 10 recite “a configuration tool for use in configuring security software packages” comprising, *inter alia*: (1) “a description logic database engine”; (2) “a security goal database associated with the description logic database”; (3) “an event database associated with the description logic database”; (4) “a first configuration module...for configuring intrusion blocking security software packages”; (5) “a second configuration module...for configuring intrusion detecting security software packages”; and (6) “a system hardening module...for automating a process of hardening the network.” Applicants submit that Gleichauf does not show or suggest the claimed elements for the following reasons.

In general, Gleichauf, col. 5, lines 33-57 does not show or suggest “a configuration tool for use in configuring security software packages.” Instead, Gleichauf discloses a “network security system...operable to detect attacks upon [a] network.” (See Gleichauf, col. 5, lines 43-44). Gleichauf’s disclosed network security system for detecting network attacks is not the same as Applicants’ claimed “configuration tool for use in configuring security software packages.”

First, Gleichauf, col. 5, lines 33-67 does not disclose “a description logic database engine.” Applicants’ claimed “description logic database engine” provides, *inter alia*, “active inference, such as automatic classification of classes and/or objects into a generalization hierarchy, rule firing and maintenance, inheritance, propagation and bounds constraints” and “further facilitates handling of incomplete and incrementally evolving knowledge bases.” (See

Applicants' Specification, paragraph 0017). In contrast, Gleichauf discloses using a "scan engine" that "gathers the network information" and a "protocol engine and signature engine" that "perform the analysis tasks upon the monitored traffic." (See Gleichauf, col. 5, lines 48-51). Gleichauf does not disclose a "description logic database" and none of the components of Gleichauf's disclosed system perform the functions of Applicants' claimed "description logic database engine."

Second, Gleichauf, col. 7, lines 1-65 does not disclose "a security goal database associated with the description logic database engine" for at least the reason that Gleichauf does not disclose a "description logic database engine." Moreover, Applicants' claimed "security goal database," *inter alia*: (1) "describes the uses that the equipment (hardware and software) of the network are intended to support" (See Applicants' Specification, paragraph 0023); (2) "may contain definitions of categories of network entities" (See Applicants' Specification, paragraph 0024); (3) "contains definitions of security goals" (See Applicants' Specification, paragraph 0025); (4) "contains a decomposition of high-level security goals into low-level security goals" (See Applicants' Specification, paragraph 0026); and (5) may "facilitate a higher order security policy, or security meta-policy" (See Applicants' Specification, paragraph 0027). In contrast, Gleichauf discloses making available "to another process or a system administrator," "the results of the protocol analysis provided by protocol engine and signature analysis provided by the signature engine...recorded in storage." (See Gleichauf, col. 7, lines 17-21). Gleichauf's disclosed "results of protocol analysis...and signature analysis" is not the same as Applicants' claimed "security goal database" and nothing in Gleichauf's disclosed system performs the functions of Applicants' claimed "security goal database."

Additionally, Gleichauf, col. 5, lines 52-67 and col. 6, lines 1-15, does not show or suggest “an event database associated with the description logic database engine” for at least the reason the Gleichauf does not disclose a description logic database. Also, Gleichauf col. 6, lines 50-67 and col. 7, lines 1-25 does not show or suggest “a first configuration module...for configuring intrusion blocking security software packages”; “a second configuration module...for configuring intrusion detecting security software packages”; or “a system hardening module...for automating a process of hardening the network.”

Therefore, Applicants submit that Gleichauf fails to show or suggest all of the elements recited in claims 4 and 10. Accordingly, Applicants submit that claims 4 and 10 are allowable over Gleichauf for at least the reasons above. Claims 5-9 depend from claim 4. Applicants further submit that claims 5-9 are allowable for at least the reason that they depend from an allowable claim.

**(c) Claims 11-16**

Claims 11 and 15 recite a method for configuring a security software package installed on an individual network device comprising, *inter alia*, “using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device.” Applicants submit that Gleichauf does not show or suggest the claimed elements for the following reasons.

Gleichauf, col. 5, lines 1-50 does not disclose the step of “using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device.” The cited portions of Gleichauf disclose different options for installing a network security system relative to other network devices and firewalls, where the “network security system is operable to

detect attacks” on the network by using a “scan engine” to obtain network information and a “protocol engine and signature engine” to analyze traffic on the network. (See Gleichauf, col. 5, lines 1-50). Placing a security system at different locations within a network to detect network attacks is nothing like Applicants’ claimed step of “using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device.”

Therefore, Applicants submit that Gleichauf fails to show or suggest all of the elements recited in claims 11 and 15. Accordingly, Applicants submit that claims 11 and 15 are allowable over Gleichauf for at least the reasons above. Claims 12-14 depend from claim 11 and claim 16 depends from claim 15. Applicants further submit that claims 12-14 and claim 16 are allowable for at least the reason that these claims depend from an allowable claim.

**(d) Claims 17-20**

Claims 17 and 18 recite “a method for configuring a security software package” comprising, *inter alia*: (1) “defining one or more security policies for a class of network devices, wherein the security software package is a service running on at least one network device of the class of network devices”; (2) “using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals”; and (3) “using a database engine providing deduction to associate the one or more security goals with the at least one network devices.” Applicants submit that Gleichauf does not show or suggest the claimed elements for the following reasons.

Gleichauf, col. 6, lines 12-45 does not show or suggest “defining one or more security policies for a class of network devices, wherein the security software package is a service running on at least one network device of the class of network devices.” Instead, the portion of

Gleichauf cited by the Examiner describes: (1) a “scan engine” that “sends a request to a domain mapping service” to obtain a “network map comprising a compilation of network information”; (2) a “protocol engine” that “performs a plurality of protocol analyses upon monitored traffic...to detect attacks upon the network”; and (3) a “signature engine” that “compares monitored traffic with attack signatures” so as “to detect attacks upon [the] network.” None of any of Gleichauf’s disclosed “scan engine,” “protocol engine,” or “signature engine” perform the claimed step of “defining one or more security policies for a class of network devices.”

Gleichauf, col. 5, lines 32-67 and col. 6, lines 1-67 does not show or suggest the steps of “using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals” or “using a database engine providing deduction to associate the one or more security goals with the at least one network devices” at least because Gleichauf does not disclose a “database engine providing deduction.” (See Section 2(a), second paragraph above).

Therefore, Applicants submit that Gleichauf fails to show or suggest all the elements recited in claims 17 and 18. Accordingly, Applicants submit that claims 17 and 18 are allowable over Gleichauf for at least the reasons above. Claims 19 and 20 depend from claim 18. Applicants further submit that claims 19 and 20 are allowable for at least the reason they depend from an allowable claim.

### 3. Conclusion

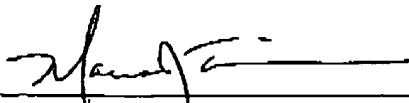
Applicants submit that the present application is in condition for allowance, and notice to that effect is hereby requested. Should the Examiner feel that further dialog would advance the

subject application to issuance, the Examiner is invited to telephone the undersigned at (312) 913-0001.

Respectfully submitted,

Dated: August 16, 2006

By:

  
\_\_\_\_\_  
Marcus J. Thymian  
Reg. No. 43,954